Honors Theory of Computation, G22.3550, Spring 2002; Yap; May 13, 2002.

FINAL EXAM (with SOLUTION)

ANSWER ALL QUESTIONS. THIS IS AN OPEN BOOK, IN-CLASS EXAM. PLEASE WRITE ONLY IN COMPLETE ENGLISH SENTENCES.

1. (Short Questions, 10 Points Each)
   Brief justification is necessary; you may cite any known results. DO NOT write more than half a page for any part of this question (often 2 lines suffice).

   (a) TRUE/FALSE: $L = \{a^n b^{2n} a^n : n \in \mathbb{N}\}$ is context-free.
   (b) Draw the quantum circuit to produce the following state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ starting from $|000\rangle$.
   (c) The following three statements cannot all be true:
   (i) All reversible gates are quantum gates.
   (ii) The control-NOT gate named T_2 can copy any bit x, i.e., $T_2(|x, 0\rangle) = |x, x\rangle$.
   (iii) The No Cloning Theorem is true.
   What is the apparent contradiction? Resolve it.

   SOLUTION:
   (a) FALSE: Here is a proof by contradiction. (The question is tricky because L looked like some other languages known to be a CFL.) Assuming L is CFL, then the pumping lemma says that if $x \in L$ has length sufficiently long, then $x = uvwyz \in L$ such that for all $i \in \mathbb{N}$, $uv^i wy^i z \in L$. Clearly, vy must contain both a's and b's. If v contain a's and b's, then $v^2 = \ldots b \ldots a \ldots b \ldots$, which implies v^2 is not s subword of x. Contradiction.
   (b) You may recall that we can produce $(|00\rangle + |11\rangle)/\sqrt{2}$ using a Hadamdard gate on line 1, then use a control-NOT (or T_2) gate on line 2 (using line 1 as control line). Simply follow this circuit by another control-NOT gate applied to line 3 (using line 1 as control gate again).
   (c) The seeming contradiction comes from (ii) saying that you can clone a bit, and (iii) saying you cannot. Moreover, (i) tells you that you can regard the gate in (ii) as a quantum gate. The resolution lies in the fact that statement (ii) is only true when x is a classical state!

2. (Reduction, 20 Points)
   Suppose $A \in NP \cap$co-NP. Show that if B is Cook-reducible to A then $B \in NP \cap$co-NP.

   SOLUTION: Let A be accepted by an NP-machine M_0 and co-A be accepted by a NP-machine M_1. Suppose T is a deterministic oracle machine that reduces B to A. We construct an NP-machine (call it N) to accept B as follows: on any input x, we simulate T until a query z is made. At that moment, we dovetail a computation of M_0 on z, and a computation of M_1 on z. If M_0 accepts, we continue the simulation of T from the "yes" state of the query machine. If M_1 acccepts, we continue the simulation of T from the "no" state. We accept iff T accepts. It is clear that N accepts x iff $T^{(A)}$ accepts x. Hence $B \in NP$.

   We also show that $B \in$ co-NP. Construct a nondeterministic machine N' that is similar to N above. Only difference is that if N accepts, then we reject, and vice-versa.

3. (Kolmogorov Complexity, 20 Points)
Let $A \subseteq \mathbb{N}$. We say A is **sparse** if there is a constant $C > 0$ such that for all n large enough, $|\{x : x \in A, x < 2^n\}| < n^C$. Give an upper bound on the function $f(n) = K(\chi_A[n]|n)$ when A is a sparse and recursively enumerable. Here, $\chi_A[n] = \langle b_0 b_1 \cdots b_{n-1} \rangle$ where $b_i = 1$ iff $i \in A$.

SOLUTION: (This is essentially Barzdin's theorem for sparse set, and the proof is exactly as for a similar homework problem!)

We claim that $K(\chi[n]|n) \leq \ell(\ell(n)) + C$ for some C.

Let N be any deterministic Turing machine that accepts A. Construct a STM M that on input $\langle n, m \rangle$, will dovetail the computations of N on the inputs $i = 0, 1, \ldots, n-1$. When m of these computations accepts, then N outputs a string $b_0 b_1 \cdots b_n$ where $b_i = 1$ iff the acceptor for A has accepted i.

Note that M will loop if less than m of the computations of N accept. Clearly, if $\chi_A[n]$ has m 1's, then our machine N on $\langle n, m \rangle$ will output $\chi_A[n]$. But by sparseness of A, $\chi_A[n]$ has $m \leq \lg(n^c) = c \lg n$ non-zero entries. Thus, $K_N(\chi_A[n]|n) = \ell(m) \leq \ell(\ell(n)) + c_0$, for some c_0. By invariance, $K(\chi_A[n]|n) \leq \ell(\ell(n)) + C$ for some C.

4. (Choice Computation, 20 Points)
Describe a polynomial time alternating machine that, on input (n, x, r), will accept iff r is the n-order of x, i.e., $x \in \mathbb{Z}_n^*$ and $\mathtt{ord}_n(x) = r$. You may assume that checking whether a number is prime is in *NP*.

Give an algorithm with as few alternations as possible (one alternation suffice). What is the number of alternations in your solution (you must explain your algorithm clearly enough that this number is easy to see)?

SOLUTION:

On input (n, x, r), we first check that $\mathtt{GCD}(n, x) = 1$ and that $x^r \equiv 1 (\mathrm{mod}\, n)$. All this in polynomial time. If check fails, we answer NO, else we continue. Then we universally guess $s < r$ and check that $x^s \not\equiv 1 (\mathrm{mod}\, n)$. If so, we reply YES.

There is only one alternation "round" in this answer. (Note: your answer should justify some of the above assertions, etc)

5. (Quantum Computation, 40 Points)
Let U be a unitary transformation and $|v\rangle$ an eigenvector such that $U|v\rangle = \omega^\phi |v\rangle$ where $0 \leq \phi < 1$ and, as usual, we write ω for $e^{\mathbf{i} 2\pi}$.

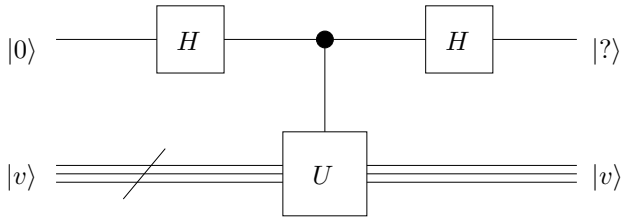

Figure 1: Alternative primitive for phase estimation

(i) Consider the circuit in Figure 1 that has two Hadamard gates and a control-U gate. What is the output of this circuit on input $|0\rangle \otimes |v\rangle$?
(ii) Show that the probability of $|0\rangle$ on the control line is $p_0 = (1 + \cos 2\pi\phi)/2$.
(iii) Suppose X is the number of heads in n tosses of a coin. If the coin has probability p $(0 < p < 1)$ of showing up heads, then

$$\Pr\{|p - (X/n)| > \varepsilon\} \leq 2\exp(-2n\varepsilon^2).$$

This is known as the "Hoeffding bound". Suppose $\cos 2\pi\phi = 0.b_1b_2b_3\cdots$ in binary notation. Using the Hoeffding bound as well as the quantum circuit, describe an experimental procedure to estimate the first two bits b_1, b_2 so that

$$\Pr\{|\cos 2\pi\phi - 0.b_1b_2| > 1/8\} \leq \delta \tag{1}$$

where $0 < \delta < 1$ is given.
(iv) Outline a generalization of (iii), so that we efficiently estimate the first m bits of $\cos 2\pi\phi$ with error probability δ. That is, $\Pr\{|\cos 2\pi\phi - 0.b_1b_2\cdots b_m| > 2^{m+1}\} \leq \delta$. HINT: use the control-$U^{2^i}$ circuits $(i \geq 1)$ to estimate the bits in parallel.

SOLUTION:
(i) Begin with the state $|0\rangle \otimes |v\rangle$. After the first Hadamard gate, we get $(|0\rangle + |1\rangle) \otimes |v\rangle/\sqrt{2}$. After applying control-U, we obtain $(|0\rangle + \omega^\phi|1\rangle) \otimes |v\rangle/\sqrt{2}$. After the second Hadamard gate, we get

$$((|0\rangle + |1\rangle) + \omega^\phi(|0\rangle + |1\rangle)) \otimes |v\rangle/2 = ((1 + \omega^\phi)|0\rangle + (1 - \omega^\phi)|1\rangle) \otimes |v\rangle/2.$$

(ii) The probability of $|0\rangle$ is $|1+\omega^\phi|^2/4 = (1+\omega^\phi)(1+\omega^{-\phi})/4 = (1+\omega^\phi+\omega^{-\phi}+\omega^0)/4 = (1 + \cos 2\pi\phi)/2$.
(iii) The idea is simply to measure the control line in this circuit n times, and if h is the number of times that we get the state $|0\rangle$, then we would like to estimate p_0 by h/n. There are two steps to reach our goal of estimating $c = \cos 2\pi\phi$. The following argument is slightly more general than what we ask you to show.

Initially let $\varepsilon > 0$ be left unspecified. This will be determined after we see what restrictions on ε are needed. Let E be the event $\{|p_0 - (h/n)| > \varepsilon\}$. We want the following bound to hold:

$$\Pr(E) = \Pr\{|p_0 - (h/n)| > \varepsilon\} \leq \delta. \tag{2}$$

Hoeffding's bound tells us that it is sufficient to choose n such that $\delta \geq 2\exp(-2n\varepsilon^2)$, or

$$n \geq \frac{1 + \ln(1/\delta)}{2\varepsilon^2}. \tag{3}$$

Next, we re-express the above event E.

$$\begin{aligned} E &= \{|p_0 - (h/n)| > \varepsilon\} \\ &= \{|(1 + c)/2 - (h/n)| > \varepsilon\}, \qquad c = \cos 2\pi\phi \\ &= \{|c - ((2h/n) - 1)| > 2\varepsilon\}. \end{aligned}$$

Thus $(2h/n) - 1$ is to be our estimate for c. Suppose we choose the bits $b_1, b_2, \ldots, b_t$ such that

$$|((2h/n) - 1) - 0.b_1 b_2 \cdots b_t| \leq 2\varepsilon.$$

This is possible provided $2\varepsilon \geq 2^{-t-1}$, or

$$\varepsilon \geq 2^{-t-2}. \tag{4}$$

We then see that

$$\begin{aligned} \{|c - 0.b_1 b_2 \cdots b_t| > 4\varepsilon\} &\subseteq \{|c - ((2h/n) - 1)| > 2\varepsilon\} \cup \{|((2h/n) - 1) - 0.b_1 b_2 \cdots b_t| > 2\varepsilon\} \\ &= \{|c - ((2h/n) - 1)| > 2\varepsilon\}, \end{aligned}$$

where the last equality follows from the fact that $\{|((2h/n) - 1) - 0.b_1 b_2 \cdots b_t| > 2\varepsilon\}$ is empty.
Hence

$$\Pr\{|c - 0.b_1 b_2 \cdots b_t| > 4\varepsilon\} \leq \Pr\{|c - ((2h/n) - 1)| > 2\varepsilon\} = \Pr(E) \leq \delta.$$

If we want to ensure that

$$\Pr\{|c - 0.b_1 b_2 \cdots b_t| > 2^{-t}\} \tag{5}$$

we just need $4\varepsilon \geq 2^{-t}$ or $\varepsilon \geq 2^{-t-2}$. Combined with (4), we can choose

$$\varepsilon = 2^{-t-2}. \tag{6}$$

From (3), we only have to choose

$$n = \left\lceil (1 + \ln(1/\delta) 2^{2t+3} \right\rceil.$$

Note that the exam question asks for the case $t = 2$ only.
(iv) This is considerably harder to do, but we would be happy if you could sketch out some of the issues that must be solved.

Before attempting the solution, the obvious question is "why not simply use the framework of part (iii)?" The answer is, yes, part (iii) can be generalized to give as many bits of precision as you like. The catch is that the number of measurements n will grow exponentially with the precision: $n = \Omega(\varepsilon^{-2})$, or $n = \Omega(4^p)$ if you want p bits of precision. Hence for efficiency, you will need to use control-U^{2^i} gates for $i = 1, 2 \ldots$, as in phase estimation.

A new complication arises: we are only estimating $\cos 2\pi\phi$, not ϕ. So when we apply U^{2^i}-gates, we are getting estimates for $\cos 2\pi\phi 2^i$. Hence you need to modify (iii) so that you directly obtain estimates on ϕ rather than $\cos 2\pi\phi$. This can be done, but requires more analysis.

We must answer the following question: if you know t bits of precision for $\cos 2\pi\phi$ (that is, you know c such that $|c - \cos 2\pi\phi| \leq 2^{-t}$), how many bits of precision do you know about ϕ? It is easy to prove the upper bound

$$|\cos(x + \delta_x) - \cos x| \leq |\delta_x|.$$

Unfortunately, what we need is a lower bound. Using Taylor series with remainder, we have

$$\cos(x + \delta_x) = \cos x - \delta_x \sin(x + \delta')$$

where $0 \leq \delta' \leq \delta_x$. Thus

$$|\cos(x + \delta_x) - \cos x| \geq |\delta_x \sin(x + \delta')|$$

This means we must first bound x away from $0, \pi, 2\pi$ (otherwise the righthand side gets arbitrarily close to 0. Assuming this has been done, so that we know some constant $c > 0$ where

$$|\cos(x + \delta_x) - \cos x| \geq \delta_x 2^{-c}$$

This means that

$$\delta_x < 2^{-t+c}.$$

At each stage $i \geq 0$, we choose $t = c + 5$ to ensures that we can estimate $2\pi\phi 2^i$ to at least 5 bits of precision, and hence $\phi 2^i$ to at least 2 bits of precision. We obtain obtain

$$\phi = 0.\phi_1\phi_2\phi_3 \cdots = \frac{\lfloor 2\phi \rfloor}{2} + \frac{\lfloor 2^2\phi \rfloor}{2^2} + \frac{\lfloor 2^3\phi \rfloor}{2^3} + \cdots.$$

FINALLY, if we want to compute ϕ to p bits of precision with error probability at most δ, we can make the error probability for estimating each bit to be δ/p. This concludes the algorithm.